

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

**MARKING OBJECT VIRTUALIZATION
INTELLIGENCE, LLC,**

Plaintiff,

v.

SYMANTEC CORPORATION,

Defendant.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Marking Object Virtualization Intelligence, LLC (“MOV Intelligence” or “Plaintiff”), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 6,802,006 (“the ‘006 patent”); 7,650,504 (“the ‘504 patent”); 7,650,418 (“the ‘418 patent”); and 7,124,114 (“the ‘114 patent”) (collectively, the “patents-in-suit” or the “MOV Intelligence Patents”). Defendant Symantec Corporation (“Symantec” or “Defendant”) infringes each of the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.*

INTRODUCTION

1. MOV Intelligence and its wholly-owned subsidiary, MOV Global Licensing LLC (“MOV Global Licensing”) pursues the reasonable royalties owed for Symantec’s unauthorized use of patented groundbreaking technology both here in the United States and throughout Europe. MOV Intelligence and its subsidiaries were assigned the rights to these patented technologies by Rovi Corporation (“Rovi”).¹

2. Rovi Corporation was a pioneer and leader in protecting computer technology, including digital rights management (“DRM”) and digital watermarking systems. Rovi assigned

¹ On April 29, 2016, Rovi Corporation acquired TiVo, Inc. The combined company operates under the name TiVo, Inc.

MOV Intelligence rights to over 233 patents including many of John O. Ryan's, the founder of Rovi predecessor Macrovision, groundbreaking patents.²

THE PARTIES

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC

3. Marking Object Virtualization Intelligence, LLC ("MOV Intelligence") is a Texas limited liability company with its principal place of business located at 903 East 18th Street, Suite 217, Plano, Texas 75074. MOV Intelligence is committed to advancing the current state of DRM and watermarking technologies.

4. MOV Intelligence Global Licensing, LLC ("MOV Global Licensing") is a wholly-owned subsidiary of MOV Intelligence and assists in the licensing of MOV Intelligence's patents in territories outside the United States with a focus on the European Union (and the United Kingdom).³ MOV Intelligence Global Licensing, LLC is a corporation organized under the laws of Delaware.

5. Rovi assigned the following patents to MOV Intelligence: U.S. Patent Nos. 7,299,209; 6,510,516; 6,802,006; 7,650,504; 6,813,640; 7,650,418; 7,200,230; 7,124,114; 6,381,367; 6,374,036; 6,360,000; 6,553,127; 6,701,062; 6,594,441; 7,764,790; 8,014,524; 6,931,536; and International Patent Nos. DE60047794; DE60148635.8; DE60211372.5; DE69901231.7-08; DK1047992; EP1047992; EP1303802; EP1332618; EP1444561; ES1047992; FR1047992; FR1303802; FR1332618; FR1444561; GB1047992; GB1303802; GB1332618; GB1444561; GR3040059; IE1047992; IE1444561; IT1047992; NL1047992; NL1444561; PT1047992; and SE1047992.

6. MOV Intelligence has the right to sublicense the following international patent assets: AT1020077; AT1198959; AT1080584; ATE232346; AT1020077; AU729762;

² See U.S. Patent Nos. 6,381,367; 7,764,790; 6,701,062; 8,014,524; German Patent Nos. DE60001837 and DE60001837D1; Chinese Patent No. CN1186941C; Canadian Patent No. CA2379992C; European Patent No. EP1198959B1; and Japanese Patent No. JP4387627B2.

³ Wolfram Schrag, *EU-Patent steht auf der Kippe*, BR.COM NACHRICHTEN (August 2016).

AU741281; AU753421; AU743639; AU714103; AU729762; AU2002351508; AU765747;
AU2000263715; BE1020077; BE1198959; BE1020077; BE1080584; BE900498; BRPI
9812908-2; BR9709332.7; BRPI 9812908-2; CA2305254; CA2332546; CA2379992;
CA2305254; CA2332548; CA2557859; CA2252726; CA2462679; CA2315212; CA2416304;
CA2425115; CH1020077; CH1080584; CH900498; CH1020077; CH1047992;
CNZL98809610.2; CNZL99806376.2; CNZL00811179.0; CNZL98809610.2;
CNZL99806377.0; CNZL97194746.5; CNZL02820738.6; CNZL99802008.7;
CNZL00819775.X; CNZL200510089437; DE69807102.608; DE60001837.7; DE69908352.4-
08; DE69718907.4-08; DE69807102.608; DK1020077; DK1080584; DK1198959; DK1020077;
DK900498; EP1020077; EP1198959; EP1080584; EP900498; EP1020077; ES1020077;
ES1198959; ES1080584; ESES2191844; ES1020077; FI1020077; FI1080584; FI1020077;
FI900498; FR1020077; FR1198959; FR1080584; FR900498; FR1020077; GB1020077;
GB1198959; GB1080584; GB900498; GB1020077; GR3041381; GR3045620; GR3043304;
GR3041381; HK1028696; HKHK1035625; HK1028696; HK1035282; HK1018562;
HKHK1069234; HKHK1057115; HK1083653B; IE1020077; IE1198959; IE1020077;
IE1080584; IE900498; IL135498; IL139543; IL148002; IL135498; IL139544; IN201442;
IN220504; IN201442; IN207829; IT1020077; IT1080584; IT900498; IT1020077; JP4139560;
JP4263706; JP4387627; JP4551617; JP4139560; JP4263706; JP3542557; JP4627809;
JP4698925; JP4366037; JP4307069; KR374920; KR422997; KR761230; KR374920;
KR362801; KR478072; KR689648; KR539987; KR752067; KR728517; KR593239;
MX223464; MX231725; MX226464; MX223464; MX212991; MX214637; MX237690;
MX240845; MYMY-123159-A; MYMY-123159-A; NL1020077; NL1198959; NL1080584;
NL900498; NL1020077; NZ503280; NZ507789; NZ503280; NZ532122; PT1010077;
PT1198959; PT1080584; PT900498; PT1010077; RU2195084; RU2216121; RU2251821;
RU2195084; RU2208301; RU2258252; SE1020077; SE1198959; SE1080584; SE900498;
SE1020077; SG71485; SG76965; SG86547; SG76964; SG71485; TWNI117461; TWNI-

124303; TWNI-130428; TWNI1600674; TWNI-162661; TWNI-202640; TWNI117461; TWNI-130754; and TWNI-184111.

SYMANTEC CORPORATION

7. On information and belief, Defendant Symantec Corporation is a Delaware corporation, with its headquarters at 20330 Stevens Creek Blvd, Cupertino, CA 95014. On information and belief, Symantec Corporation can be served through its registered agent, Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

JURISDICTION AND VENUE

8. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

9. Upon information and belief, this Court has personal jurisdiction over Symantec in this action because Symantec has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Symantec would not offend traditional notions of fair play and substantial justice. Symantec, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. In addition, Defendant Symantec is registered to do business in the State of Texas.

10. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Symantec is registered to do business in Texas, and upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

MOV INTELLIGENCE’S LANDMARK INVENTIONS

11. The groundbreaking inventions in DRM and digital watermarking taught in the patents-in-suit were pioneered by Rovi. Rovi, established in 1983 under the name Macrovision, was a trailblazing technology company focused on inventing and bringing to market fundamental technologies designed to allow producers and distributors of film and music to widely distribute their products while simultaneously protecting their art from unauthorized copying.⁴

Macrovision’s copy protection technology became so important to content creators that Congress specifically regulated the manufacture and sale of technology that was incompatible with Macrovision’s copy protection technology. *See* 17 U.S.C. § 1201(k)(1) (“unless such recorder conforms to the automatic gain control copy control technology”).⁵ Rovi broadened its focus to include copy protection and DRM for other media,⁶ including computer executables, firmware, operating system images, watermarking, and encryption.

12. MOV Intelligence’s patent portfolio, which includes more than 233 issued patents worldwide, is a direct result of Rovi’s substantial investment in research and development. The asserted MOV Intelligence patents are reflective of this history of innovation, embodying a number of firsts in the development of DRM and watermarking technologies.

13. MOV Intelligence long-term financial success depends in part on its ability to establish, maintain, and protect its proprietary technology through patents. Defendant’s

⁴ Aljean Harmetz, *Cotton Club Cassettes Coded to Foil Pirates*, N.Y. TIMES (April 24, 1985).

⁵ *See also* David Nimmer, *Back from the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 862 (2001) (The DMCA “contains a welter of corporation-specific features, relating to Macrovision Corp. The features in question relate to section 1201’s controls on consumer analog devices.”) (citations omitted).

⁶ *See* Michael Arnold et al., TECHNIQUES AND APPLICATIONS OF DIGITAL WATERMARKING AND CONTENT PROTECTION 203 (2002) (Describing Rovi’s Cactus Data Shield product which by 2002 had been used in over 100 million compact discs. “This scheme [Rovi Cactus Data Shield] operates by inserting illegal data values instead of error-correcting codes.”); *see also* Rovi *SafeDisc Copy Protection Overview*, MACROVISION CORPORATION DATASHEET at 2 (1999) (“SafeDisc incorporates a unique authentication technology that prevents the re-mastering of CD-ROM titles and deters attempts to make unauthorized copies. The SafeDisc authentication process ensures that consumers will only be able to play original discs. The user is forced to purchase a legitimate copy.”); Kirby Kish, MACROSAFE SYSTEM: A SOLUTION FOR SECURE DIGITAL MEDIA DISTRIBUTION at 7 (January 2002) (showing the architecture of the MacroSafe system and use of a DRM Server and Key Escrow Server).

infringement presents significant and ongoing damage to MOV Intelligence's business. Symantec, in an effort to expand its product base and profit from the sale of patented technology, has chosen to incorporate MOV Intelligence's fundamental technology without a license or payment.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,802,006

14. U.S. Patent No. 6,802,006 (the "'006 patent"), entitled "System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images," was filed on July 22, 1999, and claims priority to January 15, 1999. MOV Intelligence is the owner by assignment of the '006 patent. A true and correct copy of the '006 patent is attached hereto as Exhibit A. The '006 patent claims specific methods and systems for verifying the authenticity of executable images. The system includes a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified.

15. The '006 patent has been cited by over 85 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '006 patent as relevant prior art:

- Intertrust Technologies Corporation
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Check Point Software Technologies, Inc.
- Nokia Corporation
- Ipass, Inc.
- NyteLL Software LLC
- Amazon Technologies, Inc.
- Panasonic Corporation
- Matsushita Electric Ind. Co. Ltd.
- NXP B.V. (now Cisco Systems, Inc.)

- Intel Corporation
- Hewlett-Packard Development Company, L.P.
- Apple, Inc.
- Lockheed Martin Corporation
- ***Symantec Corporation***
- Zone Labs, Inc.

16. The '006 patent claims a technical solution to a problem unique to computer systems: verifying and authenticating executable images.

U.S. PATENT NO. 7,650,504

17. U.S. Patent No. 7,650,504 (the “‘504 patent”), entitled “System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images,” was filed on August 23, 2004, and claims priority to July 22, 1999. MOV Intelligence is the owner by assignment of the ‘504 patent. A true and correct copy of the ‘504 patent is attached hereto as Exhibit B. The ‘504 patent claims specific methods and systems for verifying the authenticity of executable images. The systems and methods taught in the ‘504 patent incorporate a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified. In addition, the validator ensures that each of the pointers in the executable image have not been improperly redirected.

18. The ‘504 patent and its underlying application have been cited by over 30 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘504 patent as relevant prior art:

- Qualcomm Incorporated
- Intel Corporation
- Micro Beef Technologies, Ltd
- Microsoft Corporation
- Apple, Inc.
- ***Symantec Corporation***
- Samsung Electronics Co., Ltd.
- Cybersoft Technologies, Inc.

- Electronics and Telecommunications Research Institute (ETRI)

19. The '504 patent claims a technical solution to a problem unique to the transmission of digital information over a network: verifying the identity of a software application in a dynamic loading environment. In particular, the system determines whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

U.S. PATENT NO. 7,650,418

20. U.S. Patent No. 7,650,418 (the "'418 patent'"), entitled "System and Method for Controlling the Usage of Digital Objects," was filed on August 26, 2004, and claims priority to December 8, 1998. MOV Intelligence is the owner by assignment of the '418 patent. A true and correct copy of the '418 patent is attached hereto as Exhibit C. The '418 patent claims specific methods and systems for controlling the usage of digital objects wherein control rights associated with a digital data object activate an external control object and an intercept application to intercept and monitor communications between a hosting application and a document server application associated with the creation of the digital data object. The '418 patent teaches the use of intercepting and monitoring functions without affecting or changing the hosting application or the document server application. The external control object activates an intercept application which mimics the functions of the document server application and performs user actions on the digital data object as authorized by the external control object according to the control rights associated with the digital object. By intercepting and monitoring user actions on a digital data object, the invention can control access and use of the digital data object.

21. The '418 patent family has been cited by over 47 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '418 patent as relevant prior art:

- Google, Inc.
- Fisher-Rosemount Systems, Inc.
- Knoa Software, Inc.
- Securewave S.A.
- International Business Machines Corporation

- Ab Initio Technology LLC
- The Invention Science Fund I, LLC
- Searete LLC
- Microsoft Corporation

22. The '418 patent claims a technical solution to a problem unique to the transmission of digital information over a network: reliably controlling the usage of digital objects wherein the system and/or methods intercept the communication between two applications communicating over a computer network.

U.S. PATENT NO. 7,124,114

23. U.S. Patent No. 7,124,114 (the "'114 patent'"), entitled "Method and Apparatus for Determining Digital A/V Content Distribution Terms Based on Detected Piracy Levels," was filed on November 9, 2000. MOV Intelligence is the owner by assignment of the '114 patent. A true and correct copy of the '114 patent is attached hereto as Exhibit D. The '114 patent claims specific methods and systems for distributing copyrighted material over a computer network. Specifically, the '114 patent teaches the providing of protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient; and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms. The '114 patent also discloses the use of a first set of program code which serves to ascertain terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient. The first set of program code also serves to provide or withhold a copy of the protected material to or from the prospective recipient in accordance with the terms.

24. The '114 patent family has been cited by over 39 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '114 patent as relevant prior art:

- Google, Inc.
- NBCUniversal Media, Inc.
- Digimarc Corporation

- Hewlett-Packard Development Company, L.P.
- Aigo Research Institute of Image Computing Co., Ltd.
- AT&T Intellectual Property I, L.P.
- General Electric Company
- The Nielsen Company (US), LLC
- Sca Ipla Holdings, Inc.
- Thomson Licensing, Inc.
- Fujitsu Limited

25. The '114 patent claims a technical solution to a problem unique to the transmission of digital information over a network: preventing the unauthorized copying of digital content. The patent teaches the use of a server that manages access to content according to terms determined from information stored in a database of prior unauthorized copying attributed to that recipient.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,802,006

26. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

27. Symantec designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for determining the authenticity of an executable image.

28. Symantec designs, makes, sells, offers to sell, imports, and/or uses Symantec Ghost Solution Suite 3.1; Symantec Ghost Solution Suite 3.0; and Symantec Ghost Solution Suite 2.5 (the "Symantec '006 Product(s)").

29. On information and belief, one or more Symantec subsidiaries and/or affiliates use the Symantec '006 Products in regular business operations.

30. On information and belief, one or more of the Symantec '006 Products include authentication technology.

31. On information and belief, one or more of the Symantec '006 Products enable authenticating the identity of a software application in a dynamic loading environment. In particular, the Symantec '006 Products determine whether an executable image has been

dynamically connected to another data object that has been tampered with subsequent to the execution of the software application.

32. On information and belief, the Symantec '006 Products are available to businesses and individuals throughout the United States.

33. On information and belief, the Symantec '006 Products are provided to businesses and individuals located in the Eastern District of Texas.

34. On information and belief, the Symantec '006 Products enable identifying one or more locations within the executable image, each of the identified locations being modified by a program loader.

35. On information and belief, the Symantec '006 Products comprise a system wherein a reference digital signature is generated based on an executable image.

36. On information and belief, the Symantec '006 Products generate a reference digital signature that excludes one or more locations in an executable image.

37. On information and belief, the Symantec '006 Products are capable of storing the reference digital signature on a computer network.

38. On information and belief, the Symantec '006 Products comprise systems and methods wherein an authenticity digital signature is generated based on an executable image.

39. On information and belief, the Symantec '006 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

40. On information and belief, the Symantec '006 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

41. On information and belief, the Symantec '006 Products contain functionality that generates a warning if the reference digital signature does not match the authenticity digital signature.

42. On information and belief, the Symantec '006 Products contain functionality wherein the digital signature is generated based on a first and second point in time. For example, one or more of the Symantec '006 Products generate a reference digital signature at a first point in time. Subsequently, an authenticity digital signature is generated (at a second point in time).

43. On information and belief, the Symantec '006 Products comprise a system and method that generates a digital signature based on a hash value. Specifically, the reference digital signature that is generated by the Symantec '006 Products at a first point in time is based on a hash value. Later the authenticity digital signature is also generated based on a hash function that is used to check data integrity.

44. On information and belief, the Symantec '006 Products comprise a system and method that can verify the identity a computer application.

45. On information and belief, the Symantec '006 Products enable the detection of corrupted data in a computer image.

46. On information and belief, the Symantec '006 Products enable the verification of the integrity of software images.

47. On information and belief, Symantec has directly infringed and continues to directly infringe the '006 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Symantec '006 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the Symantec '006 Products.

48. By making, using, testing, offering for sale, and/or selling verification and authentication products and services, including but not limited to the Symantec '006 Products, Symantec has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '006 patent, including at least claims 1, 3, 14, and 15, pursuant to 35 U.S.C. § 271(a).

49. On information and belief, Symantec also indirectly infringes the '006 patent by actively inducing infringement under 35 USC § 271(b).

50. On information and belief, Symantec had knowledge of the '006 patent since at least November 4, 2014 based on Symantec's citation of the '006 patent as relevant prior art in the prosecution history of U.S. Patent No. 8,881,287, entitled "Systems and methods for library function identification in automatic malware signature generation." In the alternative, Symantec has had knowledge of the '006 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Symantec knew of the '006 patent and knew of its infringement, including by way of this lawsuit.

51. On information and belief, Symantec intended to induce patent infringement by third-party customers and users of the Symantec '006 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Symantec specifically intended and was aware that the normal and customary use of the accused products would infringe the '006 patent. Symantec performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '006 patent and with the knowledge that the induced acts would constitute infringement. For example, Symantec provides the Symantec '006 Products that have the capability of operating in a manner that infringe one or more of the claims of the '006 patent, including at least claims 1, 3, 14, and 15, and Symantec further provides documentation and training materials that cause customers and end users of the Symantec '006 Products to utilize the products in a manner that directly infringe one or more claims of the '006 patent. By providing instruction and training to customers and end-users on how to use the Symantec '006 Products in a manner that directly infringes one or more claims of the '006 patent, including at least claims 1, 3, 14, and 15, Symantec specifically intended to induce infringement of the '006 patent. On information and belief, Symantec engaged in such inducement to promote the sales of the Symantec '006 Products, *e.g.*, through Symantec user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '006 patent. Accordingly, Symantec has induced and continues to induce users of the

accused products to use the accused products in their ordinary and customary way to infringe the '006 patent, knowing that such use constitutes infringement of the '006 patent.

52. The '006 patent is well-known within the industry as demonstrated by the over 85 citations to the '006 patent in issued patents and published patent applications assigned to technology companies and academic institutions. Several of Symantec's competitors have paid considerable licensing fees for their use of the technology claimed by the '006 patent. In an effort to gain an advantage over Symantec's competitors by utilizing the same licensed technology without paying reasonable royalties, Symantec infringed the '006 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

53. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '006 patent.

54. As a result of Symantec's infringement of the '006 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Symantec's infringement, but in no event less than a reasonable royalty for the use made of the invention by Symantec together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,650,504

55. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

56. Symantec designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for verifying the authenticity of executable images.

57. Symantec designs, makes, sells, offers to sell, imports, and/or uses the Symantec Ghost Solution Suite 3.1; Symantec Ghost Solution Suite 3.0; and Symantec Ghost Solution Suite 2.5 (the "Symantec '504 Product(s)").

58. On information and belief, one or more Symantec subsidiaries and/or affiliates use the Symantec '504 Products in regular business operations.

59. On information and belief, one or more of the Symantec '504 Products include authentication technology.

60. On information and belief, one or more of the Symantec '504 Products comprise systems and methods for determining the authenticity of an executable image.

61. On information and belief, one or more of the Symantec '504 Products enable authenticating and verifying an executable image. In particular, the Symantec '504 Products determine whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

62. On information and belief, the Symantec '504 Products are available to businesses and individuals throughout the United States.

63. On information and belief, the Symantec '504 Products are provided to businesses and individuals located in the Eastern District of Texas.

64. On information and belief, the Symantec '504 Products enable the use of a reference digital signature for an executable image. The reference digital signature uses the contents of the executable image excluding portions of the executable that are fixed-up by a program loader.

65. On information and belief, the Symantec '504 Products comprise a system wherein a reference digital signature is generated based on an executable image.

66. On information and belief, the Symantec '504 Products generate a reference digital signature that excludes one or more locations in an executable image.

67. On information and belief, the Symantec '504 Products comprise systems and methods wherein subsequent to the loading of the executable image the '504 Products determine an authenticity digital signature to verify that the executable image has not been improperly modified.

68. On information and belief, the Symantec '504 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

69. On information and belief, the Symantec '504 Products are systems and methods that generate an authenticity digital signature after the executable image is loaded into memory. The authenticity digital signature which is generated by the Symantec '504 Products excludes one or more pointers in need of fixing up;

70. On information and belief, the Symantec '504 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

71. On information and belief, the Symantec '504 Products enable the generating of a reference digital signature prior to loading the executable image into memory. Specifically, the Symantec '504 Products generate a reference digital signature that excludes one or more pointers from the reference digital signature.

72. On information and belief, the Symantec '504 Products contain functionality wherein the digital signature is generated based on a first and second point in time.

73. On information and belief, the Symantec '504 Products have the ability to compare the reference digital signature and the authenticity digital signature to perform an authenticity check.

74. On information and belief, the Symantec '504 Products enable the detection of corrupted data in a computer image.

75. On information and belief, the Symantec '504 Products enable the verification of the integrity of software images.

76. On information and belief, Symantec has directly infringed and continues to directly infringe the '504 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Symantec '504 Products,

which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the Symantec ‘504 Products.

77. By making, using, testing, offering for sale, and/or selling authentication and verification technologies and services, including but not limited to the Symantec ‘504 Products, Symantec has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘504 patent, including at least claims 1 and 10, pursuant to 35 U.S.C. § 271(a).

78. On information and belief, Symantec also indirectly infringes the ‘504 patent by actively inducing infringement under 35 USC § 271(b).

79. On information and belief, Symantec had knowledge of the ‘504 patent since at least November 4, 2014 based on Symantec’s citation of the ‘504 patent as relevant prior art in the prosecution history of U.S. Patent No. 8,881,287, entitled “Systems and methods for library function identification in automatic malware signature generation.” In the alternative, Symantec has had knowledge of the ‘504 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Symantec knew of the ‘504 patent and knew of its infringement, including by way of this lawsuit.

80. On information and belief, Symantec intended to induce patent infringement by third-party customers and users of the Symantec ‘504 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Symantec specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘504 patent. Symantec performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘504 patent and with the knowledge that the induced acts would constitute infringement. For example, Symantec provides the Symantec ‘504 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘504 patent, including at least claims 1 and 10, and Symantec further provides documentation and training materials that cause customers and end users of the Symantec ‘504 Products to utilize the

products in a manner that directly infringe one or more claims of the '504 patent. By providing instruction and training to customers and end-users on how to use the Symantec '504 Products in a manner that directly infringes one or more claims of the '504 patent, including at least claims 1 and 10, Symantec specifically intended to induce infringement of the '504 patent. On information and belief, Symantec engaged in such inducement to promote the sales of the Symantec '504 Products, e.g., through Symantec user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '504 patent. Accordingly, Symantec has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '504 patent, knowing that such use constitutes infringement of the '504 patent.

81. The '504 patent is well-known within the industry as demonstrated by the over 30 citations to the '504 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Apple, Inc. and Electronics and Telecommunications Research Institute (ETRI)). Several of Symantec's competitors have paid considerable licensing fees for their use of the technology claimed by the '504 patent. In an effort to gain an advantage over Symantec's competitors by utilizing the same licensed technology without paying reasonable royalties, Symantec infringed the '504 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

82. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '504 patent.

83. As a result of Symantec's infringement of the '504 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Symantec's infringement, but in no event less than a reasonable royalty for the use made of the invention by Symantec together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,650,418

84. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

85. Symantec designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for controlling the usage of digital objects.

86. Symantec designs, makes, sells, offers to sell, imports, and/or uses the Symantec CloudSOC (the “Symantec ‘418 Product(s)”).⁷

87. On information and belief, one or more Symantec subsidiaries and/or affiliates use the Symantec ‘418 Products in regular business operations.

88. On information and belief, one or more of the Symantec ‘418 Products comprise systems and methods for intercepting a communication between two applications in a computer environment.

89. On information and belief, one or more of the Symantec ‘418 Products enable intercepting a communication between two applications where the first and second application communicate via a predefined communications channel.

90. On information and belief, the Symantec ‘418 Products are available to businesses and individuals throughout the United States.

91. On information and belief, the Symantec ‘418 Products are provided to businesses and individuals located in the Eastern District of Texas.

92. On information and belief, the Symantec ‘418 Products include systems and methods that comprise a discreet intercept technology component (DIT) and a dynamic connection logic component (DCL).

93. On information and belief, the Symantec ‘418 Products comprise systems and methods wherein the DIT component permits the interception of communication and data flows between two or more components in component-based applications.

⁷ See SYMANTEC CLOUDSOC PRODUCT PAGE, available at: <https://www.elastica.net/cloudsoc/> (last visited September 2016).

94. On information and belief, the Symantec '418 Products enable the DIT component to be inserted between two digital components. The DIT then intercepts the data and communications, thereby controlling the communication between the two digital components.

95. On information and belief, the Symantec '418 Products comprise systems and methods that enable a control object capable of specifying a dynamic control logic depending on the intercepted data communication.

96. On information and belief, the Symantec '418 Products enable applying by the intercept application the dynamic control logic specified by the control object on the digital object.

97. On information and belief, the Symantec '418 Products contain functionality for intercepting data communication between a first application and a second application within a computer network without changing the functionality of the first application and the second application.

98. On information and belief, Symantec has directly infringed and continues to directly infringe the '418 patent by, among other things, making, using, offering for sale, and/or selling digital rights technology, including but not limited to the Symantec '418 Products, which include infringing technology for controlling the usage of data objects. Such products and/or services include, by way of example and without limitation, the Symantec CloudSOC Product.

99. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Symantec '418 Products, Symantec has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, pursuant to 35 U.S.C. § 271(a).

100. On information and belief, Symantec also indirectly infringes the '418 patent by actively inducing infringement under 35 USC § 271(b).

101. On information and belief, Symantec had knowledge of the '418 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Symantec knew of the '418 patent and knew of its infringement, including by way of this lawsuit.

102. On information and belief, Symantec intended to induce patent infringement by third-party customers and users of the Symantec '418 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Symantec specifically intended and was aware that the normal and customary use of the accused products would infringe the '418 patent. Symantec performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '418 patent and with the knowledge that the induced acts would constitute infringement. For example, Symantec provides the Symantec '418 Products that have the capability of operating in a manner that infringe one or more of the claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, and Symantec further provides documentation and training materials that cause customers and end users of the Symantec '418 Products to utilize the products in a manner that directly infringe one or more claims of the '418 patent. By providing instruction and training to customers and end-users on how to use the Symantec '418 Products in a manner that directly infringes one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, Symantec specifically intended to induce infringement of the '418 patent. On information and belief, Symantec engaged in such inducement to promote the sales of the Symantec '418 Products, e.g., through Symantec user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '418 patent. Accordingly, Symantec has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '418 patent, knowing that such use constitutes infringement of the '418 patent.

103. The '418 patent is well-known within the industry as demonstrated by the over 47 citations to the '418 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Google, Inc. and International Business

Machines Corporation). Several of Symantec's competitors have paid considerable licensing fees for their use of the technology claimed by the '418 patent. In an effort to gain an advantage over Symantec's competitors by utilizing the same licensed technology without paying reasonable royalties, Symantec infringed the '418 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

104. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '418 patent.

105. As a result of Symantec's infringement of the '418 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Symantec's infringement, but in no event less than a reasonable royalty for the use made of the invention by Symantec together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,124,114

106. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

107. Symantec designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

108. Symantec designs, makes, sells, offers to sell, imports, and/or uses the Symantec Endpoint Protection Versions 12.1.1; 12.1.2; 12.1.3; 12.1.4; 12.1.5; 12.1.6; and Symantec Endpoint Protection Cloud (the "Symantec '114 Product(s)").

109. On information and belief, one or more Symantec subsidiaries and/or affiliates use the Symantec '114 Products in regular business operations.

110. On information and belief, one or more of the Symantec '114 Products include content protection and content access technology.

111. On information and belief, one or more of the Symantec '114 Products enable providing or withholding access to digital content in accordance with digital rights management protection terms.

112. On information and belief, the Symantec '114 Products are available to businesses and individuals throughout the United States.

113. On information and belief, the Symantec '114 Products are provided to businesses and individuals located in the Eastern District of Texas.

114. On information and belief, the Symantec '114 Products enable the distribution of protected digital data.

115. On information and belief, the Symantec '114 Products comprise systems and methods wherein the Symantec '114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

116. On information and belief, the Symantec '114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms.

117. On information and belief, Symantec has directly infringed and continues to directly infringe the '114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Symantec '114 Products, which include infringing digital rights management technologies. Such products and/or services include, by way of example and without limitation, the Symantec '114 Products.

118. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the Symantec '114 Products, Symantec has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, pursuant to 35 U.S.C. § 271(a).

119. On information and belief, Symantec also indirectly infringes the '114 patent by actively inducing infringement under 35 USC § 271(b).

120. On information and belief, Symantec had knowledge of the '114 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Symantec knew of the '114 patent and knew of its infringement, including by way of this lawsuit.

121. On information and belief, Symantec intended to induce patent infringement by third-party customers and users of the Symantec '114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Symantec specifically intended and was aware that the normal and customary use of the accused products would infringe the '114 patent. Symantec performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '114 patent and with the knowledge that the induced acts would constitute infringement. For example, Symantec provides the Symantec '114 Products that have the capability of operating in a manner that infringe one or more of the claims of the '114 patent, including at least claims 1, 21, 41, and 52, and Symantec further provides documentation and training materials that cause customers and end users of the Symantec '114 Products to utilize the products in a manner that directly infringe one or more claims of the '114 patent. By providing instruction and training to customers and end-users on how to use the Symantec '114 Products in a manner that directly infringes one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, Symantec specifically intended to induce infringement of the '114 patent. On information and belief, Symantec engaged in such inducement to promote the sales of the Symantec '114 Products, e.g., through Symantec user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '114 patent. Accordingly, Symantec has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '114 patent, knowing that such use constitutes infringement of the '114 patent.

122. The '114 patent is well-known within the industry as demonstrated by the over 39 citations to the '114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image Computing Co., Ltd. and General Electric Company). Several of Symantec's competitors have paid considerable licensing fees for their use of the technology claimed by the '114 patent. In an effort to gain an advantage over Symantec's competitors by utilizing the same licensed technology without paying reasonable royalties, Symantec infringed the '114 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

123. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '114 patent.

124. As a result of Symantec's infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Symantec's infringement, but in no event less than a reasonable royalty for the use made of the invention by Symantec together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff MOV Intelligence respectfully requests that this Court enter:

- A. A judgment in favor of Plaintiff MOV Intelligence that Symantec has infringed, either literally and/or under the doctrine of equivalents, the '006 patent, the '504 patent, the '418 patent, and the '114 patent;
- B. An award of damages resulting from Symantec's acts of infringement in accordance with 35 U.S.C. § 284;
- C. A judgment and order finding that Defendant's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.
- D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant.
- E. Any and all other relief to which MOV Intelligence may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, MOV Intelligence requests a trial by jury of any issues so triable by right.

Dated: September 28, 2016

Respectfully submitted,

/s/ Dorian S. Berger

Elizabeth L. DeRieux (TX Bar No. 05770585)

D. Jeffrey Rambin (TX Bar No. 00791478)

CAPSHAW DERIEUX, LLP

114 E. Commerce Ave.

Gladewater, Texas 75647

Telephone: 903-845-5770

E-mail: ederieux@capshawlaw.com

E-mail: jrambin@capshawlaw.com

Dorian S. Berger (CA SB No. 264424)

Daniel P. Hipskind (CA SB No. 266763)

BERGER & HIPSKIND LLP

1880 Century Park East, Ste. 815

Los Angeles, CA 95047

Telephone: 323-886-3430

Facsimile: 323-978-5508

E-mail: dsb@bergerhipskind.com

E-mail: dph@bergerhipskind.com

*Attorneys for Marking Object Virtualization
Intelligence, LLC*